IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

JOSEPH DOSREIS, individually and on behalf of all others similarly situated, ***Plaintiff*,** **v.** **KRISPY KREME DOUGHNUT CORPORATION,** ***Defendant.***	Case No.: _ **JURY TRIAL DEMANDED** **CLASS ACTION COMPLAINT**

CLASS ACTION COMPLAINT

Plaintiff Joseph Dosreis ("Plaintiff"), on behalf of himself and all others similarly situated, by and through his undersigned counsel, brings this Class Action Complaint against Defendant Krispy Kreme Doughnut Corporation ("Krispy Kreme" or "Defendant") due to its failure to protect Plaintiff's personal information ("Data Breach" or "Breach"). Plaintiff alleges the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

PARTIES, JURISDICTION & VENUE

1. Plaintiff is a resident and citizen of Jacksonville, Florida which is located within Duval County.

2. Plaintiff is a former employee of Defendant, having worked for Defendant. Plaintiff has received a letter giving notification of the Data Breach and the unauthorized distribution of Plaintiff's data.[1] Specifically, Plaintiff's "name, date of birth, driver's license or state ID number,

[1] Ex. A: "Data Breach Notice Letter"

health insurance information, medical or health information, Social Security number, and username and password" were leaked.[2]

3. Defendant is a food and beverage company with its headquarters located at 2116 Hawkins Street, Suite 101, Charlotte, NC 28203.[3]

4. Defendant requires individuals, such as employees and customers, to provide them with sensitive Personal Identifying Information ("PII"), which includes, inter alia, customer and employees' full name, address, Social Security number, driver's license or state ID number, financial account and payment card information, in order to administer services.

5. Defendant collected and stored Plaintiff and the proposed Class Members' Private Information on their information technology computer systems.

6. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

7. Upon information and belief, Defendant made promises and representations to individuals', including Plaintiff and Class Members, that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.

8. As a result of collecting and storing the Private Information of Plaintiff and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff and the Class Members' Private Information from disclosure to third parties.

[2] Ex. A.
[3] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/0c411aee-5d5d-45bc-b6ad-ec41ce2bfdda.html

9. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C.§1332, because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000.00, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from each Defendant.

10. This Court has personal jurisdiction over Defendant because Defendant maintains their principal places of business in this District, regularly conduct business in this District, and have sufficient minimum contacts in this District.

11. Venue is proper under 28 U.S.C §1391(b) because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

STATEMENT OF FACTS

12. Plaintiff brings this class action against Defendant for their failure to properly secure and safeguard the sensitive personally identifiable information ("PII") of over 160,000 individuals.[4]

13. Defendant is a corporation that specializes in the sale of donuts and other breakfast items.[5]

14. Upon information and belief, Defendant collects personal data in connection with employment applications or as needed for human resources administration, or as needed in the process of selling items to customers. Such information may include the following: date of birth; Social Security Number; ethnicity, nationality, gender, and other demographic information.

[4] https://www.securitymagazine.com/articles/101711-krispy-kreme-data-breach-update-160-000-individuals-affected
[5] https://www.krispykreme.com/about

15. Defendant requires individuals to provide them with sensitive Private Information Personal Information, which includes, inter alia, customer and employees' full name, address, Social Security number, driver's license or state ID number, financial account and payment card information, in order to administer services.

16. Defendant collected and stored Plaintiff and the proposed Class Members' Private Information on their information technology computer systems.

17. Upon information and belief, Defendant made promises and representations to individuals', including Plaintiff and Class Members, that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.

18. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's PII was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the PII from those risks left the data in a dangerous condition.

19. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

20. On or around November 19, 2024, or November 29, 2024, a third party gained access to Defendant's corporate systems and data ("Breach" or "Data Breach").[6] The Breach was discovered on May 22, 2025.[7]

[6] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/0c411aee-5d5d-45bc-b6ad-ec41ce2bfdda.html ; Ex. A
[7] Id.

21. Upon information and belief, the following types of Private Information may have been compromised as a result of the Data Breach: full name, address, Social Security number, driver's license or state ID number, financial account and payment card information.

22. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

23. The Data Breach was a direct result of Defendant's failure to implement an information security program designed to: (a) to ensure the security and confidentiality of employee information; (b) to protect against anticipated threats or hazards to the security or integrity of that information; and (c) to protect against unauthorized access to that information that could result in substantial harm or inconvenience to any employee.

24. Defendant admits that an unauthorized third party accessed their IT Network. Defendant failed to take adequate measures to protect their computer systems against unauthorized access.[8]

25. As a result of collecting and storing the Private Information of Plaintiff and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff and the Class Members' Private Information from disclosure to third parties.

26. An information security program encompasses the administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information. Had Defendant implemented an information security program consistent with industry standards and best practices, it could have prevented the Data Breach.

[8] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/0c411aee-5d5d-45bc-b6ad-ec41ce2bfdda.html

27. As a result of the Data Breach, Plaintiff has suffered an actual injury, similar to an intangible harm remedied at common law. Defendant's failure to implement an information security program resulted in the unauthorized disclosure of Plaintiff's private information to cybercriminals. The unauthorized disclosure of Plaintiff's PII constitutes an invasion of a legally protected privacy interest, that is traceable to the Defendant's failure to adequately secure the PII in its custody, and has resulted in actual, particularized, and concrete harm to the Plaintiff. The injuries Plaintiff suffered, as described herein, can be redressed by a favorable decision in this matter.

28. Defendant has not provided any assurances that: all data acquired in the Data Breach, or copies thereof, have been recovered or destroyed; or, that Defendant has modified its data protection policies, procedures, and practices sufficient to avoid future, similar, data breaches.

29. Defendant's conduct, as evidenced by the circumstances of the Data Breach, has created a substantial risk of future identity theft, fraud, or other forms of exploitation.

30. The imminent risk of future harm resulting from the Data Breach is traceable to the Defendant's failure to adequately secure the PII in its custody, and has created a separate, particularized, and concrete harm to the Plaintiff.

31. More specifically, the Plaintiff's exposure to the substantial risk of future exploitation caused or will cause them to: (i) spend money on mitigation measures like credit monitoring services and/or dark web searches; (ii) lose time and effort spent responding to the Data Breach; and/or (iii) experience emotional distress associated with reviewing accounts for fraud, changing usernames and passwords or closing accounts to prevent fraud, and general

anxiety over the consequences of the Data Breach. The harm Plaintiff's suffered can be redressed by a favorable decision in this matter.

32. Armed with the PII acquired in the Data Breach, data thieves have already engaged in theft and can, in the future, commit a variety of crimes including, opening new financial accounts, taking out loans, using Plaintiff's information to obtain government benefits, file fraudulent tax returns, obtain driver's licenses, and give false information to police during an arrest.

33. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases." [9] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[10]

34. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[11]

---

[9] *See*, https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.

[10] *Id.*

[11] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf

35. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[12] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[13]

36. Note, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

37. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[14]

38. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft. *Portier v. NEO Tech. Sols*., No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant . . . . Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc*., 2021 WL 860584, at

[12] *See* https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/
[13] *See* https://www.investopedia.com/terms/s/ssn.asp
[14] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft

*4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiff's Social Security numbers are: arguably "the most dangerous type of personal information in the hands of identity thieves" because it is immutable and can be used to "impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and] employment." . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] social security number derives its value in that it is immutable," and when it is stolen it can "forever be wielded to identify [the victim] and target his in fraudulent schemes and identity theft attacks.")

39. Similarly, the California state government warns consumers that: "[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."[15]

40. As a result of the Data Breach, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and increased risk their PII will be further misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access on the dark web or otherwise; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the data.

[15] *See* https://oag.ca.gov/idtheft/facts/your-ssn

41. Plaintiff brings this class action lawsuit individually, and on behalf of all those similarly situated, to address Defendant's inadequate data protection practices and for failing to provide timely and adequate notice of the Data Breach.

42. Through this Complaint, Plaintiff seeks to remedy these harms individually, and on behalf of all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiff has a continuing interest in ensuring that personal information is kept confidential and protected from disclosure, and Plaintiff should be entitled to injunctive and other equitable relief.

Data Breaches Are Avoidable

43. Upon information and belief, the Data Breach was a direct result of Defendant's failure to: (i) identify risks and potential effects of collecting, maintaining, and sharing personal information; (ii) adhere to its published privacy practices; (iii) implement reasonable data protection measures for the collection, use, disclosure, and storage of personal information; and/or (iv) ensure its third-party vendors were required to implement reasonable data protection measures consistent with Defendant's data protection obligations.

44. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's PII was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the PII from those risks left the data in a dangerous condition.

45. Upon information and belief, the Data Breach occurred as the result of a ransomware attack. In a ransomware attack, the attackers use software to encrypt data on a compromised network, rendering it unusable and then demand payment to restore control over

the network.[16] Ransomware groups frequently implement a double extortion tactic, "where the cybercriminal **posts portions of the data** to increase their leverage and force the victim to pay the ransom, and then sells the stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[17]

46. To detect and prevent cyber-attacks, Defendant could and should have implemented the following measures:

Reasonable Safeguards

a. Regularly patch critical vulnerabilities in operating systems, software, and firmware on devices. Consider using a centralized patch management system.
b. Check expert websites (such as www.us-cert.gov) and your software vendors' websites regularly for alerts about new vulnerabilities and implement policies for installing vendor-approved patches to correct problems.
c. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks. Depending on your circumstances, appropriate assessments may range from having a knowledgeable employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit.
d. Scan computers on your network to identify and profile the operating system and open network services. If you find services that you don't need, disable them to prevent hacks or other potential security problems.
e. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
f. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email.
g. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
h. Configure firewalls to block access to known malicious IP addresses.
i. Set anti-virus and anti-malware programs to conduct regular scans automatically.

[16] *Ransomware FAQs*, https://www.cisa.gov/stopransomware/ransomware-faqs (accessed June 11, 2024).
[17] *Ransomware: The Data Exfiltration and Double Extortion Trends*, https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (accessed June 11, 2024).

j. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

k. Configure access controls—including file, directory, and network share permissions— with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

l. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

m. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

n. Consider disabling Remote Desktop protocol (RDP) if it is not being used.

o. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

p. Execute operating system environments or specific programs in a virtualized environment.

q. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

r. Conduct an annual penetration test and vulnerability assessment.

s. Secure your backups.[18]

t. Identify the computers or servers where sensitive personal information is stored.

u. Identify all connections to the computers where you store sensitive information. These may include the internet, electronic cash registers, computers at your branch offices, computers used by service providers to support your network, digital copiers, and wireless devices like smartphones, tablets, or inventory scanners.

v. Don't store sensitive consumer data on any computer with an internet connection unless it's essential for conducting your business.

w. Encrypt sensitive information that you send to third parties over public networks (like the internet) and encrypt sensitive information that is stored on your computer network, laptops, or portable storage devices used by your employees. Consider also encrypting email transmissions within your business.

x. Regularly run up-to-date anti-malware programs on individual computers and on servers on your network.

[18] *How to Protect Your Networks from Ransomware*, at p.3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (accessed June 11, 2024).

y. Restrict employees' ability to download unauthorized software. Software downloaded to devices that connect to your network (computers, smartphones, and tablets) could be used to distribute malware.

z. To detect network breaches when they occur, consider using an intrusion detection system.

aa. Create a "culture of security" by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities.

bb. Tell employees about your company policies regarding keeping information secure and confidential. Post reminders in areas where sensitive information is used or stored, as well as where employees congregate.

cc. Teach employees about the dangers of spear phishing—emails containing information that makes the emails look legitimate. These emails may appear to come from someone within your company, generally someone in a position of authority. Make it office policy to independently verify any emails requesting sensitive information.

dd. Before you outsource any of your business functions investigate the company's data security practices and compare their standards to yours.[19]

47. Given that Defendant collected, used, and stored PII, Defendant could and should have identified the risks and potential effects of collecting, maintaining, and sharing personal information.

48. Without identifying the potential risks to the personal data in Defendant's possession, Defendant could not identify and implement the necessary measures to detect and prevent cyberattacks. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of Plaintiff's and the Class Members' PII.

49. Defendant knew and understood unencrypted PII is valuable and highly sought after by cybercriminals seeking to illegally monetize that data. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable

[19] *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (accessed June 19, 2025).

consequences that would occur if a data breach occurred, including the significant cost that would be imposed on Plaintiff and the Class Members as a result.

Plaintiff and Class Members Sustained Damages in the Data Breach

50. The invasion of the Plaintiff and Class Members' privacy suffered in this Data Breach constitutes an actual, particularized, redressable injury traceable to the Defendant's conduct. As a consequence of the Data Breach, Plaintiff and Class Members sustained monetary damages that exceed the sum or value of $5,000,000.00.

51. Additionally, Plaintiff and Class Members face a substantial risk of future identity theft, fraud, or other exploitation where their names and social security numbers were targeted by a sophisticated hacker known for stealing and reselling sensitive data on the dark web. The substantial risk of future identity theft and fraud created by the Data Breach constitutes a redressable injury traceable to the Defendant's conduct.

52. Upon information and belief, a criminal can easily link data acquired in the Data Breach with information available from other sources to commit a variety of fraud related crimes. An example of criminals piecing together bits and pieces of data is the development of "Fullz" packages.[20] With "Fullz" packages, cyber-criminals can combine multiple sources of PII to apply for credit cards, loans, assume identities, or take over accounts.

53. Given the type of targeted attack in this case, the sophistication of the criminal claiming responsibility for the Data Breach, the type of PII involved in the Data Breach, the

[20] "Fullz" is term used by cybercriminals to describe "a package of all the personal and financial records that thieves would need to fraudulently open up new lines of credit in a person's name." A Fullz package typically includes the victim's name, address, credit card information, social security number, date of birth, bank name, routing number, bank account numbers and more. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm

hacker's behavior in prior data breaches, the ability of criminals to link data acquired in the Data Breach with information available from other sources, and the fact that the stolen information has been placed, or will be placed, on the dark web, it is reasonable for Plaintiff and the Class Members to assume that their PII was obtained by, or released to, criminals intending to utilize the PII for future identity theft-related crimes or exploitation attempts.

54. The substantial risk of future identity theft, fraud, or other exploitation that Plaintiff and Class Members face is sufficiently concrete, particularized, and imminent that it necessitates the present expenditure of funds to mitigate the risk. Consequently, Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to understand and mitigate the effects of the Data Breach.

55. For example, the Federal Trade Commission has recommended steps that data breach victims take to protect themselves and their children after a data breach, including: (i) contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity); (ii) regularly obtaining and reviewing their credit reports; (iii) removing fraudulent charges from their accounts; (iv) closing new accounts opened in their name; (v) placing a credit freeze on their credit; (vi) replacing government-issued identification; (vii) reporting misused Social Security numbers; (viii) contacting utilities to ensure no one obtained cable, electric, water, or other similar services in their name; and (ix) correcting their credit reports.[21]

56. As a consequence of the Data Breach, Plaintiff and Class Members sustained or will incur monetary damages to mitigate the effects of an imminent risk of future injury. The

[21] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps

retail cost of credit monitoring and identity theft monitoring can cost around $200 a year. The cost of dark web scanning and monitoring services can cost around $180 per year.

57. As a result of the Data Breach, Plaintiff and Class Members' PII, which has an inherent market value in both legitimate and illegitimate markets, has been damaged and diminished by its unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

58. Personal information is of great value, in 2019, the data brokering industry was worth roughly $200 billion.[22] Data such as name, address, phone number, and credit history has been sold at prices ranging from $40 to $200 per record.[23] Sensitive PII can sell for as much as $363 per record.[24]

59. Furthermore, Defendant's poor data security practices deprived Plaintiff and Class Members of the benefit of their bargain. By transacting business with Plaintiff and Class Members, collecting their PII, using their PII for profit or to improve the ability to make profits, and then permitting the unauthorized disclosure of the PII, Plaintiff and Class Members were deprived of the benefit of their bargain.

60. When agreeing to be employed by Defendant or pay Defendant for products or services, consumers understood and expected that they were, in part, paying for the protection

---

[22] *Column: Shadowy data brokers make the most of their invisibility cloak*, https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[23] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

[24] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

of their personal data, when in fact, Defendant did not invest the funds into implementing reasonable data security practices. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

CLASS ACTION ALLEGATIONS

61. Plaintiff brings this nationwide class action individually, and on behalf of all similarly situated individuals, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

62. The Class that Plaintiff seeks to represent is defined as follows:

Nationwide Class: All individuals residing in the United States whose PII was accessed and acquired by an unauthorized party as a result of the Data Breach (the "Class").

Florida Subclass

All individuals residing in the State of Florida whose PII was accessed and acquired by an unauthorized party as a result of the Data Breach (the "Florida Subclass").

63. Collectively, the Class and Florida Subclass are referred to as the "Classes" or "Class Members."

64. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

65. Plaintiff reserves the right to amend the definitions of the Classes or add a Class or Subclass if further information and discovery indicate that the definitions of the Classes should be narrowed, expanded, or otherwise modified.

66. Numerosity: The members of the Classes are so numerous that joinder of all members is impracticable, if not completely impossible. While the exact number of Class Members is unknown to Plaintiff at this time and such number is exclusively in the possession of Defendant.

67. Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting solely individual members of the Classes. The questions of law and fact common to the Classes that predominate over questions which may affect individual Class Members, includes the following:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;
b. Whether Defendant had a duty not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;
c. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;
d. Whether Defendant required its third-party vendors to adequately safeguard the PII of Plaintiff and Class Members;
e. When Defendant actually learned of the Data Breach;
f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;
h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
i. Whether Defendant adequately addressed and fixed the practices, procedures, or vulnerabilities which permitted the Data Breach to occur;
j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;
k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm faced as a result of the Data Breach.

68. Typicality: Plaintiff's claims are typical of those of the other members of the Classes because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Classes.

69. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.

70. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

71. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually

afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

72. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

73. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

74. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

75. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Classes, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

76. Further, Defendant has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

77. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiff and the Classes of the Data Breach;
b. Whether Defendant owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, sharing, storing, and safeguarding their PII;
c. Whether Defendant's security measures to protect its network were reasonable in light of industry best practices;
d. Whether Defendant's (or their vendors') failure to institute adequate data protection measures amounted to negligence;
e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII;
f. Whether Defendant made false representations about their data privacy practices and commitment to the security and confidentiality of customer information; and
g. Whether adherence to industry standards and best practices for protecting personal information would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I
NEGLIGENCE/WANTONNESS
(On Behalf of Plaintiff and the Class)

78. Plaintiff incorporates paragraphs 1-77 as if fully set forth herein.

79. Plaintiff brings this claim individually and on behalf of the Class Members.

80. Defendant knowingly collected, came into possession of, and maintained Plaintiff and Class Members' Private Information, and had a duty to exercise reasonable care in

safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

81. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff and Class Members' Private Information.

82. Defendant had, and continues to have, a duty to timely disclose that Plaintiff and Class Members' Private Information within their possession was compromised and precisely the types of information that were compromised.

83. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected individuals' Private Information.

84. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and their employees and customers. Defendant was in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

85. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant are bound by industry standards to protect confidential Private Information.

86. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff and Class Members' Private Information.

87. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff and Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems; and

c. Failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

88. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff and Class Members' Private Information within Defendant possession.

89. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff and Class Members' Private Information.

90. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the Private Information within Defendant possession might have been compromised and precisely the type of information compromised.

91. Defendant breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. § 45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiff and Class Members' Private Information. In violation of the FTC guidelines, inter alia, Defendant did not protect the Private Information it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of its networks' vulnerabilities; and failed to implement policies to correct security issues.

92. It was foreseeable that Defendant failure to use reasonable measures to protect Plaintiff and Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

93. It was foreseeable that the failure to adequately safeguard Plaintiff and Class Members' Private Information would result in injuries to Plaintiff and Class Members.

94. Defendant breach of duties owed to Plaintiff and Class Members caused Plaintiff and Class Members' Private Information to be compromised.

95. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiff and Class Members, their Private Information would not have been compromised.

96. As a result of Defendant's failure to timely notify Plaintiff and Class Members that their Private Information had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

97. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the

personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

98. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 77 as though fully set forth herein.

99. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Plaintiff and Class Members' Private Information. Various FTC publications and orders also form the basis of Defendant duty.

100. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff and Class Members' Private Information and by failing to comply with industry standards.

101. Defendant conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant systems.

102. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

103. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable

data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

104. As a result of Defendant negligence per se, Plaintiff and Class Members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing, and correcting the current and future consequences of the Data Breach.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

105. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 77 as though fully set forth herein.

106. Plaintiff and Class Members conferred a benefit upon Defendant by providing Defendant with their Private Information.

107. Defendant appreciated or had knowledge of the benefits conferred upon themselves by Plaintiff. Defendant also benefited from the receipt of Plaintiff and Class Members' Private Information.

108. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the Class Members' Private Information because Defendant failed to adequately protect their Private Information. Plaintiff and the proposed Class would not have provided their Private Information to Defendant had they known Defendant would not adequately protect their Private Information.

109. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by them because of their misconduct and the Data Breach they caused.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

110. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 77 as though fully set forth herein.

111. Plaintiff and the Class provided and entrusted their Private Information to Defendant. Plaintiff and the Class provided their Private Information to Defendant as part of Defendant's regular business practices.

112. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen, in return for the business services provided by Defendant. Implied in these exchanges was a promise by Defendant to ensure that the Private Information of Plaintiff and Class Members in their possession was secure.

113. Pursuant to these implied contracts, Plaintiff and Class Members provided Defendant with their Private Information. In exchange, Defendant agreed to, among other things, and Plaintiff and the Class understood that Defendant would: (1) provide services to Plaintiff and Class Members'; (2) take reasonable measures to protect the security and confidentiality of Plaintiff and Class Members' Private Information; and (3) protect Plaintiff and Class Members' Private Information in compliance with federal and state laws and regulations and industry standards.

114. Implied in these exchanges was a promise by Defendant to ensure the Private Information of Plaintiff and Class Members in their possession was only used for the agreed-upon reasons, and that Defendant would take adequate measures to protect Plaintiff and Class Members' Private Information.

115. A material term of this contract is a covenant by Defendant that they would take reasonable efforts to safeguard that information. Defendant breached this covenant by allowing Plaintiff and Class Members' Private Information to be accessed in the Data Breach.

116. Indeed, implicit in the agreement between Defendant and Plaintiff and Class Members was the obligation that both parties would maintain information confidentially and securely.

117. These exchanges constituted an agreement and meeting of the minds between the parties.

118. When the parties entered into an agreement, mutual assent occurred. Plaintiff and Class Members would not have disclosed their Private Information to Defendant but for the prospect of utilizing Defendant services. Conversely, Defendant presumably would not have taken Plaintiff and Class Members' Private Information if they did not intend to provide Plaintiff and Class Members with its services.

119. Defendant was therefore required to reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure and use.

120. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their Private Information.

121. Defendant breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' Private Information.

122. Defendant's failure to implement adequate measures to protect the Private Information of Plaintiff and Class Members violated the purpose of the agreement between the parties.

123. As a proximate and direct result of Defendant's breaches of their implied contracts with Plaintiff and Class Members, Plaintiff and the Class Members suffered damages as described in detail above.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Classes alleged herein, respectfully requests that the Court enter judgment as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff(s) as the representatives for the Classes and counsel for Plaintiff(s) as Class Counsel;

B. For an order declaring the Defendant's conduct violates the statues and causes of action referenced herein;

C. For an order finding in favor of Plaintiff and the Classes on all counts asserted herein;

D. Ordering Defendant to pay for lifetime credit monitoring and dark web scanning services for Plaintiff and the Classes;

E. For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

F. For prejudgment interest on all amounts awarded;

G. For an order of restitution and all other forms of equitable monetary relief requiring the disgorgement of the revenues wrongfully retained as a result of the Defendant's conduct;

H. For injunctive relief as pleaded or as the Court may deem proper; and

I. For an order awarding Plaintiff and the Classes their reasonable attorneys' fees and expenses and costs of suit, and any other expense, including expert witness fees; and

J. Such other relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of all claims in this Complaint and of all issues in this action so triable as of right.

Dated: June 25, 2025.

/s/ Ryan A. Valente
Paul J. Doolittle (*pro hac vice* forthcoming)
Ryan A. Valente (N.C. Bar No. 40140)
POULIN | WILLEY | ANASTOPOULO, LLC
32 Ann Street
Charleston, SC 29403
Telephone: (803) 222-2222
Fax: (843) 494-5536
Email: paul.doolittle@poulinwilley.com
teamvalente@poulinwilley.com
cmad@poulinwilley.com

Attorneys for Plaintiff and Proposed Class